https://doi.org/10.53656/str2021-4s-1-risk

Research Results
Резултати от научни изследвания

A NEW DIMENSION OF RISKS IN SPORTS: THE CYBER DOMAIN

Dr. Eyal Pinko
Bar-Ilan University (Israel)

Abstract. The digital era and the increasing technological reliance of sport are showing a new face of threat and present a new challenge to the sports organizations – assuring the cybersecurity of the organization, the event, the team. While cybersecurity is a central topic during the design and implementation of the security of major sports events for more than a decade, the sports organizations get newly introduced in the domain, and unfortunately, some happen to learn lessons painfully – by suffering a cyber-attack. The present article aims to examine different kinds of cyber threats to which sports organizations are exposed by studying the most common types of attackers, motivation, and the means used for an attack. The applied methodology includes a literature review and case study performed on cases from three types of categories: major sports events; sports administering bodies, clubs, and athletes. The results of the analysis provide systematic information about the most common attackers' types, motivations, and approaches which can be used as a foundation for further development of cybersecurity risk assessment of sports organizations.

Keywords: cybersecurity; sports organizations; sports events; cyber threats; APT28

Introduction

From an economic perspective, the sports industry is a large and growing market. The global sports market in 2020 is estimated at 388,28 billion USD with expected growth to 440,77 billion USD in 2021(Research and Markets 2021). As every other growing industry with large turnovers, this sector manages to attract the attention of criminals looking for opportunities for financial gains. With the mass digitalization, it has never been so easy for organizations in the field of sports to process a large amount of information, automate processes, engage with fans, increase sales and profits and become a victim of a mass cyber-attack which can lead to large financial losses, reputation damage and withdraw of sponsors and credibility in only a day.

Financial interests are only one of the motivation factors for groups and individuals to exercise technological capabilities on obtaining sensitive information

about an athlete, team, club, or a federation. The Olympic Games and the major sports events have always been something much more than a sports competition (Vladova 2018). Vladova (2018) describes the Olympic movement and the Olympic games as an important element of the establishment of multiculturalism and globalism with a high ethical, social and political charge. According to Grix, the Olympic Games represent "the most political sports event of all" (Grix 2013). These major events are a strong demonstration of the international power of the host nation during the whole process – from bidding and winning to hosting itself. The mega-events have been also an influential tribune for non-verbal speak-up of social, economical, and political declarations, ex. the women's rights, the refugee crises, declaring values, showing the dominance of different political orders, etc. This is what makes them an attractive arena for state-backed, activist, or terrorist organizations to manifest their soft power. And again, due to the interconnectivity, it has never been so easy to make such great damage to an event and respectively national reputation with so little investment. This threat of course is an "extra" to the many other criminal attempts for financial gains using the fans' passion, curiosity, and likelihood to jump into a cyber trap during the games.

Cybersecurity of major sports events is of general concern since the 2010 Olympic Games in Vancouver (Beaudoin and Genik 2010). The cybersecurity of athletes and sports organizations is not on public focus until the 2020 report of the National Cyber Security Centre of the UK (NCSC)[1)] on "The cyber threat on sports organizations". Almost every sports organization has a website and social media accounts, holds digital records of personal information about customers, staff, volunteers; keeps sensitive health information and statistics about its players; uses online business systems, corporate emails and process millions of financial transactions big part of which is made online via sales of tickets, merchandise, booking, etc. According to the survey conducted for the report, 70% of the sports organizations suffered a cyber-attack and around 30% of the cyber-attack incidents on sports organizations in the UK lead to direct damage with costs varying from £500 to over £100,000 per incident.

Despite the increasing risk, the possible big loss, and the serious political damage which can be caused by a cyberattack on a sports organization, we observe a relatively small amount of scientific literature dedicated to this emerging issue.

Aim

The present article aims to examine and analyze the cyber threats to which different types of sports-related organizations are exposed, to evaluate the risks and their possible impact. The present article presents a holistic outlook on the cyber vulnerability of sports organizations with the idea to provide recommendations for the prevention and protection of the informational infrastructure in sports organizations.

Methodology

For the present study has been used a complex methodology including literature review and case study analysis. The literature review is conducted through a search in scientific databases accessed through google scholar search with keywords "cybersecurity", "cyber-attacks" and "sports", "sports organizations", "Olympics", "athlete".

The information about the cases was collected from websites of international media and official documents and press releases published online in the English language. The description of the cases was built on one or more sources with the criteria as a final result to be: described a case of a cyber-attack to a sports organization or sports event, to be included information about attack vectors; results from forensic investigation; (suspected) attacker; attack means. The cases were grouped into three categories: attacks on major sports events; attacks on sports administering bodies; attacks on sports clubs and athletes. For all the cases were analyzed the means, the profile of the attacker, and the attacker's motivations to be identified the threats, risks, and cyber vulnerability of the sports organizations.

Results

This section is divided into three parts depending on the types of victims of cyber-attacks, respectively: major sports events; sports administering bodies; sports clubs, and athletes.

Major Sports Events

Because of the large size and the high political and economic importance, all the aspects of security of major sports events are a priority for the organizers. Nowadays digital solutions are used in almost every step of organizing and conducting an event which makes cybersecurity a solid pillar of the overall security and event continuity. Despite the taken measures, the events remain vulnerable.

After the doping scandals around Russia and the incredibility of its national anti-doping agency in 2015, approximately 111 Russian athletes were excluded from the 2016 Olympic and Paralympic Games in Rio (The USA Department of Justice 2018). There is a widespread belief that the ban of Russian athletes to compete under the Russian flag marks the beginning of a series of revenge-motivated attacks which aim to compromise the next mega-events in which Russia will not compete.

In September 2016 the World Anti-Doping Agency announced that through an account with access to the Anti-Doping Administration & Management System (ADAMS), a WADA database with sensitive information about athletes has been hacked (WADA 2016) by what is believed to be a Russian state-backed hackers group calling themselves "Fancy Bears" (Kirk 2016) also known as Stortium or APT28. The result of this hack is that there was leaked sensitive information about US athletes who tested positive for banned drugs but after that obtained the so-called "therapeutic use exception" (TUE) certificate. Although there is still not a

clear confirmation of who exactly stands behind the attack, it is widely believed that in this case, the hack is about political reasons. After the attack on WADA, in 2017 the International Association of Athletics Federations (IAAF) reported another attack aiming at information about the TUE stored in its servers. In its press release[2)], the Federation informs about unauthorized remote access to the IAAF network where metadata on athlete TUEs was collected. The forensic investigation points as attackers the same group of the "Fancy Bears".

Russian-hosted major events also become a target of cybercrimes. During the FIFA World Cup 2018, the security services reported the prevention of 25 million cyber-attacks[3)]. They were different in their type. One common such was phishing before the event through campaigns offering low-cost traveling to Russia for the event. By this, the criminals aimed to collect information about credit cards and personal information. Another known approach was through the promotion of malicious apps about the World Cup. Downloading the app-enabled also installation of a spyware on the devices of curious fans who wanted to watch the live stream for free. Those who stand behind the attack are supposed to be state-sponsored groups trying to discharge the games and the IT structure of the organizers (Waterfield 2018).

One of the most emblematic cyber-attacks not only in the field of major sports events but for the history of cybersecurity is the cyberattack during the 2018 Winter Olympic Games in PyeongChang. What for some of the spectators looked as a temporary hack of the Olympic website and application and some problem with the TV screens and the Wi-Fi was actually a massive attack which ran seconds before the official opening ceremony and was prepared months before. Through still unidentified attack vector a malicious file has caused the collapse of every domain controller in the Seoul data centers (the basis of the Olympic IT infrastructure), shutting all RFID systems, TV screens. The RFID-based security entry to the Olympic buildings was blocked and the official application which had the ticketing function was also broken. Despite the professional efforts of cybersecurity experts, forensic specialists, and reverse engineers, it still remains unclear who caused the attack and the reason is the sophisticated deception approach of planting false flags. What later will be called "Olympic Destroyer" according to the specialists was "the first time someone used false flags of that kind of sophistication in a significant, national-security-relevant attack...it's a harbinger of what the conflicts of the future might look like" (Greenberg 2019).

Sports Administering Bodies

One of the aims of the present paper is to show the different type of sports organizations which are vulnerable to cyber-attacks. Sports administering bodies like sports federations, associations, respective ministries have a key political and financial importance in the development of a sport on the national and international level. From here derives the interest of the attacker to such organizations. A recent example for this was reported in 2021 when was officially confirmed that in 2017

– 2018 the Swedish Sports Confederation was the subject of attack of the Russian Military Intelligence which extracted personal and medical information about the Swedish athletes[4]. In the same period, the country was putting efforts to win the hosting of the 2026 Winter Olympics.

Another notable attack is the attack on the USA National Football League during which personal data of more than 1200 football players was leaked (Brewster 2017).

Sports Clubs and athletes

Sports clubs are operating like business organizations and are vulnerable not less than them. An example of this is the cyber-attack on Manchester United which was hacked in November 2020. According to the statement of the club, the security protocols are in place and the organization managed to handle the attack before it was able to take over critical information or block important infrastructure[5].

The UK National Cyber Security Center (NCSC 2020) reveals the case of an English League football club that became a victim of a ransom attack that blocked the access of all end-user devices of the club as well as the digital equipment on the stadium. The attack was enabled by a phishing email or remote access to the CCTV system. The club refused to pay the requested amount of 400 bitcoins but nevertheless, gaining control over its own assets cost them several hundred thousand pounds.

Hacks on individuals are also not absent. In November 2020 it was reported an attack on four UK athletes during which their iCloud profiles were hacked and intimate pictures and videos were leaked on the net[6]. Attacking the UK athletes shows that not only sports teams and sports events are victims of cyber-attacks, but sportsmen, players, and team employees are also potential victims.

Discussion

After cases of different types of sports-related cyber-attacks were presented, in this section we analyze more precisely the methods used, the means of the attack, and the attacker's motivation:

– "Fancy Bears" is probably the most known attacking team mentioned in the articles of the cyber-attacks over mega-events. The Russian APT28 is famous also for hacking governments, NGOs, universities, and private companies worldwide. The Microsoft cybersecurity specialists (Burt 2019) observed that their typical methods of attack include social engineering[7] by "spear-phishing" attacks, password spray[8], exploiting internet-connected devices (Internet of Things) to shut down systems, and using both open-source and custom malware. As we can see from the other examples, these are also the most common ways for the attacker to reach his goals. The involvement of state-backed actors like APT28 in attacking sports events, administering bodies, and teams emphasizes the significance of sports as a political tool, and cyber-attacks as a tool of intelligence gathering, manipulation, psychological warfare, or propaganda.

– Both WADA and IAAF attacks demonstrate the sensitivity of players' private and medical data and their vulnerability to cyber-attacks. Those particular cases, present how together with the personal data of the athletes, there are exposed and affected the national interests of the countries they represent. Access to such a database can be used to satisfy political, ideological, or revenge interests, to wipe whole athlete's records, change them, present them to others, or use them as part of a campaign against an athlete, a team, or a nation. Those attacks can be performed using social engineering or a brute force attack[9)] against the player herself or against the team's computers and network.

– The FIFA World Cup 2018 cyber-attacks reveal an interesting attack vector, which uses "innocent" applications which can be downloaded by users from "Google Store" or "Apple Store". Malware is being implemented in those applications. Once the user is downloading and installing them, the malware goes inside her cellular phone, it sends the attacker the user's private data, such as emails, pictures, videos, contacts, notes, and even identity card numbers, credit card numbers, etc. Then the attacker can use this information to perform other cybercrimes such as identity theft, using the credit card for online shopping, taking online loans, etc.

– The 2018 Winter Olympic Games attack shows that the attackers' moves can be so sophisticated that his identity and location can remain anonymous without ever being revealed; additionally, false signs can be implemented to distract the attention and deceit. What is more, the 2018 cyber-attacks show the ability to disrupt and shut down sports events by attacking stadiums' infrastructure, sports websites, and teams' networks.

Moving the focus to the federations, sports clubs, and athletes, experts say that the rise of cyber-attacks over sports organizations is yet to come because of the great financial resource with which the sports organizations operate and the publicity and the media coverage that the attackers will gain performing the attack (Savir 2021). The enormous financial potential that comes out of cyberattacks is attracting hacktivists, criminals, amateurs, and even terrorists trying to perform cyber-attacks for their own budgets.

As it was motioned above, the attackers already have very sophisticated approaches which let them remain anonymous while achieving their goals. This is the reason why for the reviewed cases the information about the attacker's identity is just assumed. Here we will outline the typical types of attackers in the cyber domain: nation-states, terror organizations, criminals (individuals and organized criminal groups), hacktivists, amateurs, and the internal threat – individuals (employees or suppliers).

Each type of attacker has its own set of motivations to perform a cyber-attack against sports objectives. In the following table, we summarize the cyber-attacking motivations of each type of attacker against potential targets. The table can be used as a baseline for the determination of reference attack scenarios in the risk assessment process.

Table 1. Attacker types and motivations

	Players	**Teams**	**Sports administering bodies**	**Major Events**
State-backed	• Compromising national players		• Political achievements	• Intelligence collection • Chaos • Political achievements
Terrorists		• Publicity	• Publicity	• Chaos • Political achievements • Financial gain • Publicity
Criminals	• Financial gain • Affecting gambling	• Financial gain • Affecting gambling	• Financial gain	• Financial gain • Affecting gambling
Hacktivists	• Expressing position	• Chaos • Expressing position		• Chaos • Expressing position
Amateurs	• Ego • Revenge	• Ego • Revenge • Financial gain	• Ego	• Ego • Financial gain
Employees	• Revenge • Financial gain	• Revenge • Financial gain	• Revenge • Financial gain	• Financial gain

Possible impacts of their actions include direct or in-direct money loss; legal exposure (including privacy issues); reputation damage; exposure of sensitive information; political issues.

The analysis so far shows that the most common cyber-attacking vectors include:

– DDoS (Distribution Denial of Service) against websites, servers, and other cyber assets, to shut down services, create chaos, express political ideas, and as an enabler for attack aim to steal or manipulate information.

– Ransom or extortion attacks aim to steal information, create chaos and financial gains.

– Cyber misinformation and propaganda to express political ideas and influence public opinion and decision-makers.

– Different methods of brute-force attack to steal information, manipulate information, or gain other achievements.

– Social engineering attacks, using psychological manipulation, to overcome technological barriers and gain access to the objective's cyber assets.

– Attacks performed against real-time systems and Internet of Things devices, such as cameras, controllers, and sensors, to shut down or disturb major sports events.

Conclusion

The present work reflects emerging issues in the field of sport which are very lightly touched in the scientific literature so far especially in the intersection between

sports and cybersecurity. In the age of digital transformation and high technological reliance of sports, no related organization remains absolutely safe. The attackers and their motivations can be different and the impacts of their actions vary from financial losses, reputation, and legal exposure to serious crises in international relations. While the organizers of the major events consider cybersecurity as a solid part of the security, the sports administering bodies and the sports clubs are underestimating the cyber risks. This requires the international professional and scientific community to initiate and lead awareness campaigns and researches to support the sports organizations in facing these new challenges.

NOTES

1. NCSC. *The cyber threat to sports organisations*. Available at: https://www.ncsc.gov.uk/report/the-cyber-threat-to-sports-organisations (Accessed: 3 May 2021).
2. *IAAF victim of cyber attack PRESS-RELEASE World Athletics*. Available at: https://www.worldathletics.org/news/press-release/iaaf-cyber-attack (Accessed: 4 May 2021).
3. *Russia recorded 25 mln cyber attacks to disrupt 2018 FIFA World Cup from overseas*, *TASS*. Available at: https://tass.com/society/1284343 (Accessed: 4 May 2021).
4. Business Standard, 2021. 'Swedish sports body hacked by Russian military intelligence, officials say', *Business Standard India*, 13 April. Available at: https://www.business-standard.com/article/sports/swedish-sports-body-hacked-by-russian-military-intelligence-officials-say-121041300969_1.html (Accessed: 3 May 2021).
5. *Manchester United hit by 'sophisticated' cyber attack but say fan data is safe*, *the Guardian*. Available at: http://www.theguardian.com/football/2020/nov/20/manchester-united-confirm-cyber-attack-but-confident-match-can-go-ahead (Accessed: 30 May 2021).
6. WION WebTeam, 2020. *Private pictures of four female British athletes posted online in widespread cyberattack*, *WION*. Available at: https://www.wionews.com/sports/private-pictures-of-four-female-british-athletes-posted-online-in-widespread-cyberattack-344718 (Accessed: 30 May 2021).
7. Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
8. Password spraying is an attack that attempts to access a large number of accounts (usernames) with a few commonly used passwords.
9. A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly. These attacks are done by 'brute force' meaning they use excessive forceful attempts to try and 'force' their way into private account.

REFERENCES

Beaudoin, L. and Genik, L., 2010. *Review and Coordination of Cyber Security for Vancouver 2010*. Defence Research and Development Canada.

Brewster, T., 2017. *1,200 Football Players' Personal Data Exposed In NFL Leak -- Colin Kaepernick Included*, *Forbes*. Available at: https://www.forbes.com/sites/thomasbrewster/2017/10/03/colin-kaepernick-nfl-data-leaked-hackers-ransomware-threat/ [Accessed: 30 May 2021].

Greenberg, A., 2019. 'Inside Olympic Destroyer, the Most Deceptive Hack in History', *Wired*. Available at: https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/ [Accessed: 4 May 2021].

Grix, J., 2013. 'Sport Politics and the Olympics', *Political Studies Review*, **11**(1), 15–25. doi: 10.1111/1478-9302.12001.

Kirk, J., 2016. *Hackers Dump US Olympic Athletes' Drug-Testing Results*. Available at: https://www.bankinfosecurity.com/hackers-dump-us-olympic-athletes-drug-testing-results-a-9397 [Accessed: 4 May 2021].

Reasearch and Markets, 2021. *Global Sports Market Report (2021 to 2030) – COVID-19 Impact and Recovery*, *GlobeNewswire News Room*. Available at: https://www.globenewswire.com/fr/news-release/2021/03/18/2195540/28124/en/Global-Sports-Market-Report-2021-to-2030-COVID-19-Impact-and-Recovery.html [Accessed: 31 May 2021].

Savir, M., 2021. *The growing importance of cybersecurity in sports*. Available at: https://blog.infront.sport/cybersecurity-sports [Accessed: 3 May 2021].

The USA Department of Justice, 2018. *U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations*. Available at: https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and [Accessed: 29 May 2021].

Vladova, I., 2018. *Multikulturalizam. Olimpizam. Obrazovanie.* 1st edn. Sofia: NSA-Press. [in Bulgarian]

WADA, 2016 *WADA Confirms Attack by Russian Cyber Espionage Group (13 September 2016)*, *World Anti-Doping Agency*. Available at: https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group [Accessed: 4 May 2021].

Waterfield, P., 2018. *Russia Fends Off 25 Million Cyber-Attacks During World Cup*, *Infosecurity Magazine*. Available at: https://www.infosecurity-magazine.com:443/news/russia-fends-off-25-million-world/ [Accessed: 4 May 2021].

✉ **Dr. Eyal Pinko**
https://orcid.org/0000-0002-9102-3560
IIMSR, Bar-Ilan University
Ramat Gan, Israel
E-mail: eyal.pinko@gmail.com